

WHAT IS CLAIMED IS:

- 1 1. A method of managing invalid password attempts, said
2 method comprising:
3 receiving a message from a computer system, wherein
4 the message includes a distinguished name, the
5 distinguished name corresponding to a failed
6 login attempt;
7 calculating a total failed login attempt number
8 corresponding to the distinguished name;
9 identifying a failed login attempt allowed number;
10 determining whether the total failed login attempt
11 number is greater than the failed login attempt
12 allowed number; and
13 revoking a password corresponding to the distinguished
14 name based on the determination.
- 1 2. The method as described in claim 1 wherein the message
2 is received from a plurality of servers.
- 1 3. The method as described in claim 1 further comprising:
2 establishing a secure connection with the computer
3 system; and
4 verifying a digital certificate corresponding to the
5 computer system, wherein the digital certificate
6 is included in the message.
- 1 4. The method as described in claim 1 wherein the
2 determining further comprises:
3 configuring parameters, wherein the parameters include
4 a login tracking period;
5 storing a record in a failed login data store, the
6 record including the distinguished name and a

7 timestamp corresponding to a time the message was
8 received; and
9 removing one or more records from the failed login
10 data store in response to one or more
11 corresponding timestamps being older than the
12 tracking period.

1 5. The method as described in claim 1 wherein the
2 revoking further includes:
3 preparing a password revocation message, the password
4 revocation message identifying the distinguished
5 name; and
6 sending the password revocation message to one or more
7 login servers, wherein the login servers include
8 the computer system.

1 6. The method as described in claim 5 further comprising:
2 establishing a secure connection to each of the login
3 servers; and
4 including a digital signature identifying a sending
5 computer system in the password revocation
6 message.

1 7. The method as described in claim 5 wherein the
2 password revocation message is sent in response to
3 determining that the password was not previously
4 revoked; and
5 wherein the password revocation message is not sent in
6 response to determining that the password was
7 previously revoked.

1 8. An information handling system comprising:
2 one or more processors;

RECEIVED 1992-11-11

3 a memory accessible by the processors;
4 one or more nonvolatile storage devices accessible by
5 the processors;
6 a password managing tool to process invalid password
7 attempts, the password managing tool including:
8 means for receiving a message from a computer
9 system, wherein the message includes a
10 distinguished name, the distinguished name
11 corresponding to a failed login attempt;
12 means for calculating a total failed login
13 attempt number corresponding to the
14 distinguished name;
15 means for identifying a failed login attempt
16 allowed number;
17 means for determining whether the total failed
18 login attempt number is greater than the
19 failed login attempt allowed number; and
20 means for revoking a password corresponding to
21 the distinguished name based on the
22 determination.

1 9. The information handling system as described in claim
2 8 wherein the message is received from a plurality of
3 servers.

1 10. The information handling system as described in claim
2 8 further comprising:
3 means for establishing a secure connection with the
4 computer system; and
5 means for verifying a digital certificate
6 corresponding to the computer system, wherein the
7 digital certificate is included in the message.

1 11. The information handling system as described in claim
2 8 wherein the determining further comprises:
3 means for configuring parameters, wherein the
4 parameters include a login tracking period;
5 means for storing a record in a failed login data
6 store, the record including the distinguished
7 name and a timestamp corresponding to a time the
8 message was received; and
9 means for removing one or more records from the failed
10 login data store in response to one or more
11 corresponding timestamps being older than the
12 tracking period.

1 12. The information handling system as described in claim
2 8 wherein the revoking further includes:
3 means for preparing a password revocation message, the
4 password revocation message identifying the
5 distinguished name; and
6 means for sending the password revocation message to
7 one or more login servers, wherein the login
8 servers include the computer system.

1 13. The information handling system as described in claim
2 12 further comprising:
3 means for establishing a secure connection to each of
4 the login servers; and
5 means for including a digital signature identifying a
6 sending computer system in the password
7 revocation message.

- 1 14. A computer program product stored in a computer
2 operable media for processing invalid password
3 attempts, said computer program product comprising:
4 means for receiving a message from a computer system,
5 wherein the message includes a distinguished
6 name, the distinguished name corresponding to a
7 failed login attempt;
8 means for calculating a total failed login attempt
9 number corresponding to the distinguished name;
10 means for identifying a failed login attempt allowed
11 number;
12 means for determining whether the total failed login
13 attempt number is greater than the failed login
14 attempt allowed number; and
15 means for revoking a password corresponding to the
16 distinguished name based on the determination.
- 1 15. The computer program product as described in claim 14
2 wherein the message is received from a plurality of
3 servers.
- 1 16. The computer program product as described in claim 14
2 further comprising:
3 means for establishing a secure connection with the
4 computer system; and
5 means for verifying a digital certificate
6 corresponding to the computer system, wherein the
7 digital certificate is included in the message.
- 1 17. The computer program product as described in claim 14
2 wherein the determining further comprises:

3 means for configuring parameters, wherein the
4 parameters include a login tracking period;
5 means for storing a record in a failed login data
6 store, the record including the distinguished
7 name and a timestamp corresponding to a time the
8 message was received; and
9 means for removing one or more records from the failed
10 login data store in response to one or more
11 corresponding timestamps being older than the
12 tracking period.

1 18. The computer program product as described in claim 14
2 wherein the revoking further includes:
3 means for preparing a password revocation message, the
4 password revocation message identifying the
5 distinguished name; and
6 means for sending the password revocation message to
7 one or more login servers, wherein the login
8 servers include the computer system.

1 19. The computer program product as described in claim 18
2 further comprising:
3 means for establishing a secure connection to each of
4 the login servers; and
5 means for including a digital signature identifying a
6 sending computer system in the password
7 revocation message.

1 20. The computer program product as described in claim 18
2 wherein the password revocation message is sent in
3 response to determining that the password was not
4 previously revoked; and

FILED OCT 10 1992

5 wherein the password revocation message is not sent in
6 response to determining that the password was
7 previously revoked.

1

1

IBM CORPORATION